

## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number  
**WO 2004/054168 A1**

(51) International Patent Classification<sup>7</sup>: **H04L 9/32**

(21) International Application Number:  
PCT/IB2003/005335

(22) International Filing Date:  
21 November 2003 (21.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
0228760.5 10 December 2002 (10.12.2002) GB

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];  
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **TUYLS, Pim, T.** [BE/BE]; c/o Philips Intellectual Property & Standards,

Cross Oak Lane, Redhill, Surrey RH1 5HA (GB). **MURRAY, Bruce** [GB/GB]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

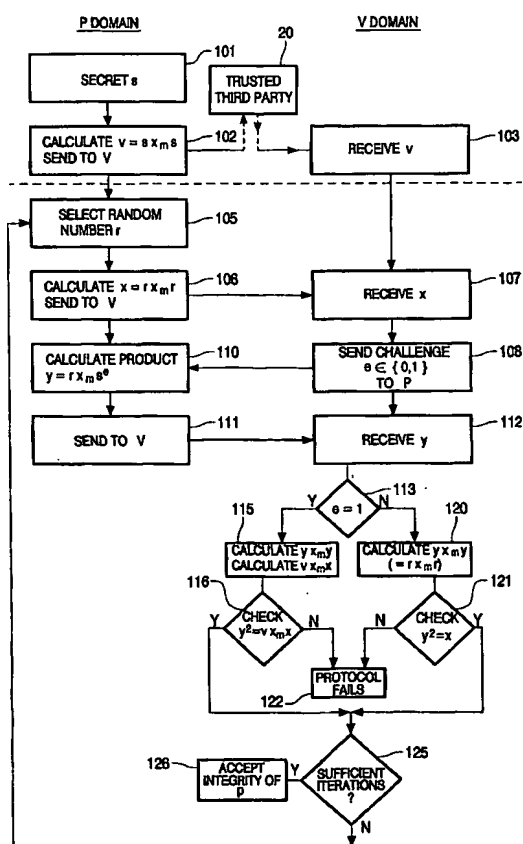
(74) Agent: **TURNER, Richard, C.**; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: EFFICIENT IMPLEMENTATION OF ZERO KNOWLEDGE PROTOCOLS



(57) Abstract: Zero knowledge protocols, such as the Fiat-Shamir and Guillou-Quisquater protocols are implemented using only Montgomery multiplications on Montgomery representations of numbers to effect a more efficient implementation of the protocols, particularly in devices that have restricted computational resource such as smart cards and other portable electronic devices.



Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,  
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE,  
SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA,  
GN, GQ, GW, ML, MR, NE, SN, TD, TG).

TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM,  
ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD,  
SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY,  
KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG,  
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT,  
LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ,  
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,  
TG)

**Declaration under Rule 4.17:**

— as to applicant's entitlement to apply for and be granted  
a patent (Rule 4.17(ii)) for the following designations AE,  
AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ,  
CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE,  
EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN,  
IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,  
MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM,  
PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ,

**Published:**

— with international search report

For two-letter codes and other abbreviations, refer to the "Guid-  
ance Notes on Codes and Abbreviations" appearing at the begin-  
ning of each regular issue of the PCT Gazette.